DOCKET FILE COPY ORIGINAL

ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED
FEB 11 1998
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

REPLY COMMENTS OF AT&T CORP.

Mark C. Rosenblum
Ava B. Kleinman
Seth S. Gross
Room 3252F3
295 North Maple Avenue
Basking Ridge, New Jersey 07920
(908) 221-4432

Roseanna DeMaria
AT&T Wireless Services
Room 1731
32 Avenue of the Americas
New York, New York 10013
(212) 830-6364

February 11, 1998

No. of Copies rec'd 0+4
List ABCDE

TABLE OF CONTENTS

SUMMARY

In its initial comments, AT&T urged the Commission to proceed carefully in this rulemaking to ensure that the Communications Assistance for Law Enforcement Act ("CALEA") is implemented as Congress intended--narrowly, efficiently and with balance. Industry overwhelming supports this approach.

In these Reply Comments, AT&T notes that not a single commenter--including the Federal Bureau of Investigation ("FBI")--suggested that compliance with CALEA by the October 1998 date was reasonably achievable. Industry comments were all in agreement that the absence of commercially available hardware or software to implement the industry's CALEA standard within the compliance period was a critical factor for the Commission to consider in making a reasonable achievability determination.

AT&T also urges the Commission to reject the FBI request that the Commission determine which costs are reasonably achievable for carriers. Congress withheld that power from the Commission in passing CALEA.

AT&T joins industry in general in requesting that the Commission issue a blanket extension of the CALEA compliance date, because CALEA-compliant hardware and software is not commercially available. AT&T also asks that the Commission make clear that commercially available under CALEA means available from the carrier's vendor, not from any third party provider of non-switch based solutions.

AT&T strongly disagrees with the FBI proposals for carrier security procedures and points out that, despite the Commission's interpretation of CALEA to the contrary, no such burdensome procedures are required. AT&T particularly objects to the FBI

proposal that the Commission require carriers to implement wiretap orders without regard to the facial validity. Finally, as all commenters agreed, CALEA does not change the scope of carrier immunity under the wiretap laws.

The Commission's use of the term "exclusively" in reference to information services that are exempt from CALEA makes it unclear whether information services provided by common carriers also are exempt as Congress intended. The Commission should make clear that all information services are exempt from CALEA whether or not such services are offered by a common carrier.

Also, as to the definition of telecommunications carrier, AT&T urges the Commission to retain its definition of common carrier as a company that holds itself out to serve the public indiscriminately. The FBI's desire to delete the term "indiscriminately" could lead to an erroneous interpretation that private carriers are covered by CALEA.

Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

REPLY COMMENTS OF AT&T CORP.

AT&T Corp. ("AT&T"), by its attorneys and pursuant to Section 1.415 of the Commission's Rules, 47 C.F.R. § 1.415, hereby submits its Reply Comments in the above-captioned proceeding in response to Comments relating to the Federal Communications Commission (the "Commission") Notice of Proposed Rulemaking regarding its responsibilities under the Communications Assistance for Law Enforcement Act ("CALEA").[1]

I. INTRODUCTION

In its comments, AT&T urged the Commission to proceed carefully in this rulemaking to ensure that CALEA is implemented as Congress intended--narrowly, efficiently and with balance.[2] On this point, as the many comments submitted to the Commission in this proceeding demonstrate, the industry overwhelmingly agrees. However, as the Commission no doubt has seen in this proceeding already, industry and the Federal Bureau of Investigation (the "FBI") comments ("FBI Comments") are at polar extremes. In these Reply Comments, any appearance that AT&T is unduly critical of the FBI and its positions in no way diminishes AT&T's

---

1 Communications Assistance for Law Enforcement Act, Notice of Proposed Rulemaking, CC Docket No. 97-213, FCC 97-356 (released October 10, 1997), Errata (released October 24, 1997) (the "NPRM").

2 Comments of AT&T, filed December 12, 1997 ("AT&T Comments"), at 1.

respect for the authority and professionalism of the FBI or its long history of cooperation with law enforcement across the nation. In this matter, AT&T simply disagrees with the breadth of CALEA interpretation proposed by the FBI. Instead, AT&T believes the Commission should interpret CALEA narrowly and consistent with Congressional intent. As the House Report states: "The Committee urges against overbroad interpretation of the requirements."[3]

II. PETITIONS UNDER REASONABLY ACHIEVABLE STANDARD

A. Compliance Will Not Be Reasonably Achievable Until Hardware and Software Is Commercially Available to Implement the Industry Standard.

In its comments, AT&T recounted the history of the development of the industry technical standard to implement the assistance capability requirements of CALEA.[4] While the standard has been available only since November 1997, manufacturers have turned to developing the necessary hardware and software for carriers to comply with the law. However, it is clear that no standardized, CALEA-compliant hardware or software will be available by October 1998, the CALEA deadline.

Not a single commenter--including the FBI--suggested that compliance by the October 1998 date was reasonably achievable. To the contrary, industry comments are all in agreement that the absence of commercially available hardware or software to implement the standard within the compliance period was a critical factor for the Commission to consider in

---

[3] See H.R. No. 103-827, at 22, reprinted in 1994 U.S.C.C.A.N. 3489, 3502 ("House Report").

[4] AT&T Comments at 2; see also, Comments of the Cellular Telecommunications Industry Association ("CTIA"), filed December 12, 1997 ("CTIA Comments"), at 2-6.

making a reasonable achievability determination.[5]

If the Commission does not recognize that the absence of commercially available, CALEA-compliant hardware and software renders compliance impracticable, carriers may opt for nonstandard implementations. As AT&T pointed out, such ad hoc solutions are neither efficient nor desirable.[6] Nonstandard implementation almost certainly will increase the cost of electronic surveillance to law enforcement, which will need to develop collection equipment to receive intercepted communications and call-identifying information from dozens of different carriers in nonstandard ways. Carriers too will bear increased costs associated with development and implementation of custom solutions.

Congress believed that CALEA could be implemented in a balanced and economical way by "designing in" the technical solutions at the outset rather than retrofitting later.[7] But the looming compliance date, coupled with the current state of standards development and implementation, almost ensures that none of the anticipated benefits will be realized, making compliance anything but reasonably achievable.[8] The Commission should act now to

---

5 See, e.g., CTIA Comments at 12; Comments of SBC Communications, Inc. ("SBC"), filed December 12, 1997 ("SBC Comments"), at 26; Comments of United States Cellular Corporation, filed December 12, 1997, at 3; Comments of the United States Telephone Association ("USTA"), filed December 12, 1997 ("USTA Comments"), at 12; Comments of U S WEST, Inc. ("USW"), filed December 12, 1997 ("USW Comments"), at 38.

6 AT&T Comments at 6-7.

7 House Report at 3515.

8 AT&T suggests that the Commission couple such a determination under Section 109 with an extension of the compliance date under Section 107. By doing so, the Commission will acknowledge the substantial effort of the industry to date in developing and implementing the recently promulgated standard while at the same time capping the amount of time the industry will have to produce the CALEA-compliant hardware and software.

acknowledge that the absence of commercially available, CALEA-compliant hardware and software renders compliance not reasonably achievable. Acting now will avoid the certain flood of carrier and manufacturer petitions seeking relief in the very near future.[9]

B. Section 109 Factors Must Be Given Equal Weight.

The Commission requested comments on the eleven factors under Section 109 that it must consider to determine whether compliance is "reasonably achievable." Like AT&T, many of those commenting referred the Commission to the clear guidance of Congress, which directed the Commission in Section 109 proceedings to (i) ensure that CALEA costs to consumers are kept low; (ii) meet the legitimate needs of law enforcement while preventing "gold-plating" of law enforcement's demands; (iii) protect subscriber privacy interests and (iv) ensure that competition in all forms of telecommunications is not undermined, ensuring that wiretap compliance is neither used as a sword or a shield.[10]

---

[9] See Comments of American Mobile Telecommunications Association, Inc., filed December 12, 1997, at 8; Comments of Bell Atlantic Mobile, Inc. ("Bell Atlantic"), filed December 12, 1997 ("Bell Atlantic Comments") at 9; Comments of BellSouth Corporation ("BellSouth"), filed December 12, 1997 ("BellSouth Comments"). at 18-19; Comments of Motorola, Inc., filed December 12, 1997 at 11; Comments of the Organization for the Promotion and Advancement of Small Telecommunications Companies, filed December 12, 1997 ("OPASTCO Comments"), at 8; Comments of PrimeCo Personal Communications, L.P., filed December 12, 1997 ("PrimeCo Comments"), at 5; Comments of the Rural Telecommunications Group, filed December 12, 1997 ("RTG Comments"), at 7; Comments of the Telecommunications Industry Association, filed December 12, 1997 ("TIA Comments"), at 10.

[10] AT&T Comments at 8 (citing 140 Cong. Rec. 10771, 10781 (October 4, 1994) (comments by Rep. Markey). See also Comments of the American Civil Liberties Union ("ACLU"), Electronic Privacy Information Center and Electronic Frontier Foundation (joint comments), filed December 12, 1997 ("ACLU Comments"); BellSouth Comments at 17.

As AT&T and BellSouth noted, a balanced approach envisioned by Congress requires that each of the factors in the Section 109(b) analysis be given equal weight.[11] And, as AT&T noted, any one factor alone could lead to a finding that compliance is not reasonably achievable.[12]

While all of the industry comments urged balance, the FBI argued, without analysis or direct support in the law, that the effect of a determination on public safety and national security "should be deemed to be the paramount consideration in the Commission's determination of reasonable achievability."[13] As AT&T noted in its comments, analysis of this factor requires more than a superficial recognition that law enforcement interests are important.[14] Instead, each case will present unique facts that the Commission must consider. Such facts will include the history of surveillance activity in an area, alternatives that a carrier could employ on a one-time or ad hoc basis to meet the immediate needs of law enforcement, and whether alternative technologies or capabilities or the facilities of another carrier are available to law enforcement to implement the surveillance. Thus, the law enforcement factor is not the "predominant" one against which all other factors must be measured.

---

11 BellSouth Comments at 17.

12 AT&T Comments at 8.

13 FBI Comments at 40.

14 AT&T Comments at 8-11.

C. The Commission Cannot Allocate Costs on Reasonable Achievability Petitions.

The Commission did not propose any procedural rules for handling petitions under Section 109, but correctly noted that if the Commission determines compliance to be not reasonably achievable, the affected carrier may petition the Attorney General and the Attorney General may agree to pay the additional, reasonable costs necessary to make compliance achievable.[15] The FBI has requested that the Commission impose certain procedural requirements, apparently by rule, even though the Commission did not propose any such requirements in the NPRM.[16] AT&T strongly objects to the FBI suggestion, and notes in addition that the procedures requested by the FBI do not comport with CALEA.

The FBI proposes that "the Commission require that individual carrier petition submissions include an estimate of the reasonable costs directly associated with the modification under consideration."[17] CALEA requires no such estimate on the part of carriers and the FBI cites no authority for the proposition. In fact, the legislative history of CALEA suggests just the opposite--that the Commission has no authority to determine *what amount* is reasonable for the carrier to pay.

As the House Report shows, Congress initially considered extending jurisdiction to the Commission to resolve disputes "regarding the amount of just and reasonable costs to be

---

15 NPRM, ¶ 46.

16 FBI Comments at 40.

17 Id..

paid."[18] Congress ultimately rejected the proposal and deleted the provision.[19] Even with the dispute resolution provision in the original bill, Congress admonished that the intent was not to permit the Commission to regulate the price of telecommunications transmission and switching equipment:

> Determinations regarding what constitutes a "reasonable charge" for modifications and features should be made in the first instance by manufacturers and their customers in contractual negotiations in accordance with normal and accepted business practices.[20]

In the end, Congress left it to the affected carrier and the Attorney General to reach an agreement on the reasonable costs of achieving compliance.[21] CALEA requires the Attorney General to promulgate regulations necessary to effectuate timely and cost-efficient payment to carriers with whom the Attorney General has reached agreement to pay.[22] The Attorney General must "prescribe regulations for purposes of determining reasonable costs."[23] Thus, it is not within the jurisdiction of the Commission to determine the "reasonable costs" a carrier should bear.

---

18 House Report at 7 (proposed section 2608(f)).

19 Although the final version of CALEA is different in a number of respects than the bill language accompanying the House Report, the House Report is the most authoritative document on the intent of Congress in passing CALEA.

20 House Report at 3510.

21 47 U.S.C. § 1008(e).

22 47 U.S.C. § 1008(e)(1). The cost-reimbursement rules are found at 28 U.S.C. § 100.9.

23 47 U.S.C. § 1008(e)(2).

Instead, any petitioning party will have to bring forth sufficient evidence that shows, overall, the cost of compliance is not reasonably achievable. The type and quantum of evidence will be determined by the factors at work in the specific petition. For example, it may be that compliance would adversely affect subscriber rates or adversely affect network operations. These sorts of petitions will not lend themselves to incremental cost estimates proposed by the FBI, and to require as much would be to rewrite CALEA.

In view of the above, the Commission also should reject the FBI recommendation that the Commission make specific findings "in terms of dollar amounts" on such petitions.[24] The Commission has no authority to determine "which costs should be assumed by the carrier, and which costs should be considered for reimbursement by the Government."[25]

D. Compliance Is Not Reasonably Achievable Without Capacity Information.

Several commenters noted that industry has yet to be informed of law enforcement's capacity requirements.[26] CALEA expressly required the Attorney General to publish its capacity requirements *not later than one year* after enactment of CALEA.[27] As the Commission notes in the NPRM, the FBI "has not yet published the rules."[28] As several

---

24 FBI Comments at 40.

25 Id..

26 See, e.g., Comments of AirTouch Communications, Inc., filed December 12, 1997 ("AirTouch Comments"), at 7; Comments of Ameritech Corporation ("Ameritech"), filed December 12, 1997 ("Ameritech Comments") at 9; BellSouth Comments at 17; RTG Comments at 7; SBC Comments at 27; USTA Comments at 13.

27 47 U.S.C. § 1003.

28 In effect, the FBI has taken a unilateral extension of the CALEA deadline for publishing this important capacity information.

commenters noted, capacity is integral to designing and implementing capability solutions,[29] and yet the capacity rules have not yet been published by the FBI.

The Commission tacitly recognizes the linkage between capacity and capability when considering requests under the reasonably achievable standard.[30] The Commission correctly notes that carriers are deemed to be in compliance with the CALEA capacity provisions "[i]f the Attorney General does not reimburse a carrier for its reasonable costs" associated with modifications of the network that are necessary to comply with capacity requirements.[31]

The FBI, however, takes the Commission to task for acknowledging the obvious, stating that the "reasonably achievable standard of CALEA does not apply to capacity compliance or reimbursement."[32] It is literally true that Section 109 determinations are based on a carrier's ability to meet Section 103 assistance requirements, not capacity requirements. However, nothing precludes the Commission from considering, as the NPRM suggests, that capacity requirements have yet to be published and that it may be more cost-efficient or desirable for a carrier to wait to

---

29 See, e.g., Ameritech Comments at 9.

30 See NPRM, ¶ 47.

31 Id.

32 FBI Comments at 39. The FBI also complains about the Commission's characterization of the FBI's first two capacity notices as being issued pursuant to rulemaking authority. FBI Comments at 39 n.34. The significance of this is unclear unless it is intended to suggest that the FBI has no obligation to respond to the significant adverse public comment regarding the two failed notices. This is also a remarkable statement given that Section 104(a)(1) of CALEA requires that the Attorney General promulgate the capacity requirements only "after notice and comment."

implement capability solutions until publication of concomitant capacity requirements.[33]

III. EXTENSION OF THE COMPLIANCE DATE

A. Section 107(c) Determinations Should Focus on Commercial Availability of Technology.

AT&T and several other commenters made clear that the purpose of Section 107 is to permit carriers to obtain an extension of the CALEA compliance date if technology necessary for compliance is not commercially available during the compliance period.[34] It was noted in these comments that the Commission proposed an incorrect standard for extensions--one based on whether compliance was "reasonably achievable," utilizing its proposed Section 109 procedures.[35]

Only after the Commission has found that CALEA-compliant hardware and software are "commercially available" should the Commission consider whether compliance is reasonably achievable. In other words, as AT&T noted in its comments, not only must there be a

---

[33] It is also worth noting that the FBI has taken the position publicly that carriers in fact are liable for the costs of capacity for all installations, deployments and significant upgrades that occur after promulgation of the final capacity notice. Industry has objected to this interpretation in comments submitted in response to the FBI's second capacity notice. That issue is not before the Commission here, but AT&T notes that if the FBI persists in this strained reading of Section 104, then it certainly would be relevant for the Commission to consider future costs of complying with capacity requirements if carriers indeed are obligated to pay despite clear Congressional guidance to the contrary. Finally, the Commission should be aware that in some cases, carriers may propose in their petitions that certain capability costs are increased significantly depending upon the architecture of the solution necessitated by capacity requirements.

[34] AT&T Comments at 24; Ameritech Comments at 8-10; Comments of Omnipoint Communications, Inc., filed December 12, 1997, at 8; USW Comments at 38-39.

[35] NPRM, ¶ 49-50.

commercially available solution, but that solution cannot otherwise be cost prohibitive.[36] At that stage of the petition proceeding, the Section 109 factors should be applied to determine whether compliance is cost-prohibitive.

The problem of focusing on the reasonably achievable clause of Section 107 is well illustrated by the FBI Comments. Section 107 requires the Commission to consult with the Attorney General prior to granting an extension request.[37] Conversely, Section 109 reasonably achievable petitions require only that the Commission give the Attorney General notice.[38] In its comments on Section 107 extensions, the FBI inexplicably argues that the "issue of reasonable achievability requires consultation with the Attorney General."[39] AT&T reiterates here its previous comments to the Commission that the FBI stands in the shoes of any other commenter on Section 109 petitions and, as such, FBI participation should be on the record.[40] Under Section 107, AT&T requested that the Commission make express, written findings of fact on each extension petition and that it address the nature and content of FBI consultations in that process.[41] This approach is critical to ensuring that the decision-making process is fair and open.

---

36 AT&T Comments at 25-26.

37 47 U.S.C. § 1006(c)(2).

38 47 U.S.C. § 1008(b)(1).

39 FBI Comments at 41.

40 AT&T Comments at 21.

41 AT&T Comments at 26-27.

B. Commercially Available, CALEA-Compliant Solutions Are Those Provided By a Carrier's Own Vendor.

The FBI asserts in its comments that the existence of some alternative "network-based, or other non-switch-based, solutions that would enable a carrier to provide certain surveillance services to law enforcement under Section 103 [. . .] would preclude the grant of an extension."[42] AT&T strongly disagrees with the implication that law enforcement can foist upon a carrier some solution that requires network redesign or the acceptance of some third-party product for integration into or attachment to its system. As Congress said in no uncertain terms,

> [L]aw enforcement agencies are not permitted to require the specific design of systems or features, nor prohibit adoption of any such design. . . . The legislation leaves it to each carrier to decide how to comply.[43]

It would be remarkable if law enforcement could obtain such a design mandate through a proceeding designed by Congress to determine when compliance is too costly. Section 107 simply does not permit law enforcement or the Commission to respond to a petition by saying "there is a cheaper or better way that involves redesigning your system."

Other commenters agree with AT&T on this critical point.[44] CALEA itself makes this clear in defining the duties of equipment manufacturers and providers of telecommunications support services:

> A telecommunications carrier shall consult, as necessary, in a timely fashion with manufacturers of its telecommunications transmission and switching

---

[42] FBI Comments at 41.

[43] House Report at 3503.

[44] See, e.g., USW Comments at 39 ("because the equipment of different manufacturers is neither compatible nor substitutable, one manufacturer's solution for providing CALEA capabilities cannot be used with the equipment of another.").

> equipment and its providers of telecommunications support services for the purpose of ensuring that current and planned equipment, facilities, and services comply with the capability requirements of section 103 and the capacity requirements identified by the Attorney General under section 104.[45]

Congress underscored the meaning of Section 106 further in the legislative history, noting that this section "requires a telecommunications carrier to consult with its own equipment manufacturers and support service providers."[46] Thus, the Commission should make clear that technology is commercially available to the petitioning carrier when that carrier's own vendor(s) has produced it and not otherwise.

C. The Comments Confirm the Need for a Two-Year Blanket Extension of the Compliance Date.

Despite the Commission's tentative decision not to address the CTIA July 1997 petition for rulemaking and extension,[47] there is overwhelming support in the comments from carriers and manufacturers for the blanket, two-year extension requested by CTIA.[48] As noted by Ameritech in its comments, the FBI itself acknowledged in its CALEA Implementation Plan, submitted to Congress on March 3, 1997, that 24 months is a reasonable time frame between adoption of a standard and implementation of technology.[49]

---

45 47 U.S.C. § 1005(a) (emphasis added).

46 House Report at 3506.

47 See NPRM, ¶ 44.

48 See, e.g., BellSouth Comments at 16; OPASTCO Comments at 6-8; TIA Comments at 9-11; ACLU Comments at 1 (extend deadline to no earlier than October 24, 2000).

49 Ameritech Comments at 9.

The large number of commenters supporting a two-year extension because technology for compliance is not available to carriers at this time should indicate to the Commission the serious need for a blanket extension today. The commenters have shown that the Commission can expect to receive individual extension requests from both carriers and manufacturers if no general extension is forthcoming. It is in the public interest to grant an extension in sufficient time to avoid the costs of filing individual petitions later.[50] Accordingly, the Commission should revisit its proposal in the NPRM to defer promulgation of specific extension request rules.[51]

IV. SYSTEMS SECURITY AND INTEGRITY

A. Appropriate Authorization Refers to a Facially Valid Surveillance Order, Which Carriers Are Required to Review.

In its comments, AT&T disagreed with the Commission's determination that CALEA's reference to "authorization" in regard to security procedures was intended to mean some form of internal carrier authorization.[52] Several commenters concurred with AT&T that "appropriate authorization" as used in Section 301 refers to the authority the carrier needs from a

---

50 It is also worth noting that a public extension request on a carrier-by-carrier basis is tantamount to announcing those systems that are or may be incapable of supporting wiretaps today. A blanket extension would avoid this problem entirely, leaving the interested criminal element in the dark about which systems currently meet or do not meet CALEA capability requirements.

51 NPRM, ¶ 50.

52 AT&T Comments at 30-31; see also NPRM, ¶ 25.

court or law enforcement officials to engage in the interception activity.[53]

The FBI, however, agreed with the Commission's assessment, but not for any security-related reason or legal analysis of the particular provision. Rather, the FBI complains about unwanted carrier scrutiny of surveillance orders and argues that if the Commission adopts its first possible reading of Section 229, then carriers will continue to scrutinize such surveillance orders in the future.[54] In a singular section of its comments, the FBI argues that

> [T]he review that a carrier gives to a court order or certificate of authorization (provided in cases of exigent circumstances) should be limited to whether (1) the court order or certification is valid on it's face (i.e., that it is what it purports to be); and, (2) the intercept is capable of being implemented as a technical matter. . . . Hence, the Commission should specify that the duty of the carrier upon receipt of a facially valid court order or statutorily-based authorization for an intercept extends only to the prompt and good faith execution of such court orders or authorizations.[55]

AT&T respectfully disagrees.[56]

Carriers are entitled to rely on the apparent lawfulness of legal process. But, carriers still must take reasonable steps to ensure that government process is consistent with statutory requirements so that only the customer information that the government is entitled to

---

53 See, e.g., Ameritech Comments at 3; CTIA Comments at 27; SBC Comments at 9-10; Comments of 360° Communications Company ("360° Communications"), filed December 12, 1997 ("360° Communications Comments"), at 2.

54 FBI Comments at 16.

55 FBI Comments at 16-17.

56 The Commission should not be caught in this briar patch. The electronic surveillance laws provide a clear answer to law enforcement's stated concerns by allowing the law enforcement agency to seek the assistance of the issuing court to enforce the surveillance order. 18 U.S.C. § 2518(8)(c) ("Any violations of the provisions of this subsection may be punished as contempt of the issuing or denying judge.").

receive is disclosed (e.g., a carrier would not permit a wiretap pursuant to a mere subpoena because a warrant is required by statute). And, carriers must ensure that they do not exceed the parameters of lawful process (e.g., continue to intercept communications after the period specified in an order or allowed by law). Otherwise, a carrier could be subjected to litigation as Congress itself has said in setting forth the basics of such a lawsuit:

> (1) The complaint must allege that a wire or electronic communications service provider (or one of its employees): (a) disclosed the existence of a wiretap; (b) acted without a facially valid court order or certification; (c) acted beyond the scope of a court order or certification or (d) acted on bad faith. Acting in bad faith would include failing to read the order or collusion. If the complaint fails to make any of these allegations, the defendant can move to dismiss the complaint for failure to state a claim upon which relief can be granted.
> (2) If during the course of pretrial discovery the plaintiff's claim proves baseless, the defendant can move for summary judgment.
> (3) If the court denies the summary judgment motion, the case goes to trial. At the close of the plaintiff's case, the defendant again can move for dismissal. If that motion is denied, the defendant then has the opportunity to present to the jury its section 2520 good faith defense.[57]

Quite obviously, Congress intended carriers to do more than blindly implement a surveillance order presented by law enforcement agencies. For example, it is not uncommon for AT&T to receive a wireless surveillance order that contains a subscriber name that does not match the electronic serial number or mobile identification number, or vice versa. Should AT&T choose blindly between the two, ask law enforcement which one they really intended, or implement taps on both? AT&T will not implement orders where there is any doubt or ambiguity about the facilities to be tapped. If there is any duty the Commission should recognize in these proceedings, it is that CALEA specifically requires carriers to protect the privacy of

---

[57] S. Rep. No. 99-541, at 26-27, reprinted in 1986 U.S.C.C.A.N. 3555, 3580-81 (emphasis added).

communications not authorized to be intercepted.[58]

The surveillance laws themselves require no less. For example, the trap and trace or pen register provisions of Title 18 require an order to specify:

- ◊ the identity, if known, of the person subject to the interception;
- ◊ the identity, if known, of the person subject to investigation;
- ◊ the number or electronic serial number of the phone subject to the installation;
- ◊ the geographical limits of the trap and trace (but not the pen register);
- ◊ a statement of the offense to which the information likely relates;
- ◊ the duration of the installation (i.e., not to exceed 60 days for federal trap and trace);[59] and
- ◊ nondisclosure instructions to the carrier.[60]

If any of the above legally required elements of a trap and trace or pen register order are missing, then the order simply may not be considered facially valid.

The FBI appears to argue that carrier concerns about incurring liability for implementing a court order containing incorrect information are misplaced.[61] The FBI states that good faith implementation of a "facially valid court order . . . all other things being equal, would provide the carrier with a defense to claims of liability."[62] The FBI does not say what things are equal or what constitutes a facially valid order. Moreover, the defense to which the FBI refers is the "good faith" defense to civil claims brought by an aggrieved person for the interception,

---

58 47 U.S.C. § 1002(a)(4)(A).

59 18 U.S.C. § 3123(b), (c).

60 18 U.S.C. § 3123(d).

61 FBI Comments at 17.

62 Id..

disclosure or intentional use of communications in violation of Title 18.[63] This defense requires a carrier to put on a case and go to the expense of litigation.

The FBI implicitly admits that carriers must do more than blindly implement court orders upon presentation. In a footnote to the above section in their comments, the FBI states that "[g]ood faith reliance on a court order . . . is a complete defense to any civil or criminal action against a carrier," citing 18 U.S.C. § 2520(d)(1), (2).[64] In effect, the FBI recognizes that it is not enough to receive and act on an order, the carrier must read and follow it in good faith.

Further, the FBI incongruously argues that, unlike when a carrier fails to read an order and improperly implements a wiretap, carrier immunity would be lost if "unauthorized interceptions" resulted from a failure to implement appropriate security procedures.[65] For the information of the Commission and the FBI, most major carrier security procedures contain specific surveillance order handling instructions to ensure that personnel do not go beyond the authorized surveillance in the order. When there is confusion based on the all-too-common typographical/numerical error, incorrect carrier corporate identity or wrong surveillance target name matched with the phone number, carriers must act in good faith to clarify the matter *before* implementing the order. Any other action might result in liability for violating a customer's privacy rights.

---

63 18 U.S.C. § 2520(d).

64 FBI Comments at 17, n.23.

65 FBI Comments at 17.

B. The Commenters Uniformly Agree That Section 105 Does Not Change the Scope of Potential Carrier Liability.

The Commission requested comment on whether its proposed security rules, recordkeeping and reporting requirements would modify or mitigate carrier liability under the wiretap laws.[66] Uniformly, commenters rejected the notion that the Commission had authority to determine vicarious liability rules or the scope of the criminal law under Title 18 of the U.S. Code.[67] Even the FBI agrees that CALEA did "not expand the potential civil or criminal liability of carriers."[68]

Section 229(d) states quite clearly that for purposes of CALEA, a violation by an officer or employee of "any policy or procedure adopted by a common carrier pursuant to subsection (b), or of a rule prescribed by the Commission pursuant to subsection (a), shall be considered to be a violation of the carrier of a rule prescribed by the Commission pursuant to this Act."[69] Obviously, the more burdensome and detailed the Commission rules, the greater the compliance challenge faced by carriers. Thus, by imposing reporting and recordkeeping obligations on carriers not mandated by CALEA, the Commission actually increases the potential

---

66 NPRM, ¶ 27.

67 See AirTouch Comments at 27; Bell Atlantic Comments at 4; BellSouth Comments at 9; Comments of GTE Service Corporation and its affiliated telecommunications companies, filed December 12, 1997 ("GTE Comments"), at 6; SBC Comments at 11; Comments of Sprint Spectrum L.P., filed December 12, 1997, at 2; USTA Comments at 7.

68 FBI Comments at 17 n. 23.

69 47 U.S.C. § 229(d).

liability of carriers--something nowhere discussed or contemplated in CALEA.[70]

C. The Commission Misinterprets the Security Requirements of CALEA.

The proposed rules by the Commission regarding carrier security procedures and policies have provoked a uniform, negative response from the industry that proposed rules are more burdensome and costly than necessary to implement the provisions of CALEA.[71] Many carriers submitted comments emphasizing that they already have internal policies and procedures that adequately address the need to ensure that intercepts are performed only when duly authorized and that the confidentiality of such surveillance activities is safeguarded.[72]

The Commission should carefully review the requirements of Section 229 before imposing this burdensome regime on carriers. Section 229 in the first instance only requires the Commission to "prescribe such rules as are necessary to implement the requirements of [CALEA]."[73] To the extent the Commission promulgates such rules, it must include rules to implement the security provisions of Section 105.[74] As AT&T noted in its comments, and as the

---

70 It is also worth noting that the discussion of vicarious liability under Title 18 is a little odd because there is some doubt about whether Title 18 authorizes a private right of action. See Cox Cable Cleveland Area, Inc. v. King, 582 F. Supp. 376 (N.D. Ohio 1983); Greek Radio Network of Am., Inc. v. Vlasopoulos, 731 F. Supp. 1227 (E.D. Pa. 1990).

71 See, e.g., AirTouch Comments at 19; Bell Atlantic Comments at 3-4; PrimeCo Comments at 6; SBC Comments at 9; USTA Comments at 6; USW Comments at 13-14.

72 AirTouch Comments at 19-20; Bell Atlantic Comments at 9; BellSouth Comments at 7-8; GTE Comments at 6-7; 360° Communications Comments at 3; SBC Comments at 17-20; Comments of Teleport Communications Group, Inc., filed December 12, 1997, at 6-7; USTA Comments at 8; USW Comments at 16-18.

73 47 U.S.C. § 229(a).

74 47 U.S.C. § 229(b).